Network Security: Challenges and Attacks

Dr Bhaskar Mondal

Cyberspace

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

-- A Definition of Cyberspace

Challenges

Innumerable entry points to internet.

easy to misdirect attribution to other parties

Protection from critical operations (missions)

Attack technology outpacing defense technology

Nation states, non-state actors, and individuals are at a peer level, all capable of waging attacks

Critical Security Challenges

Infiltrations and ransomware

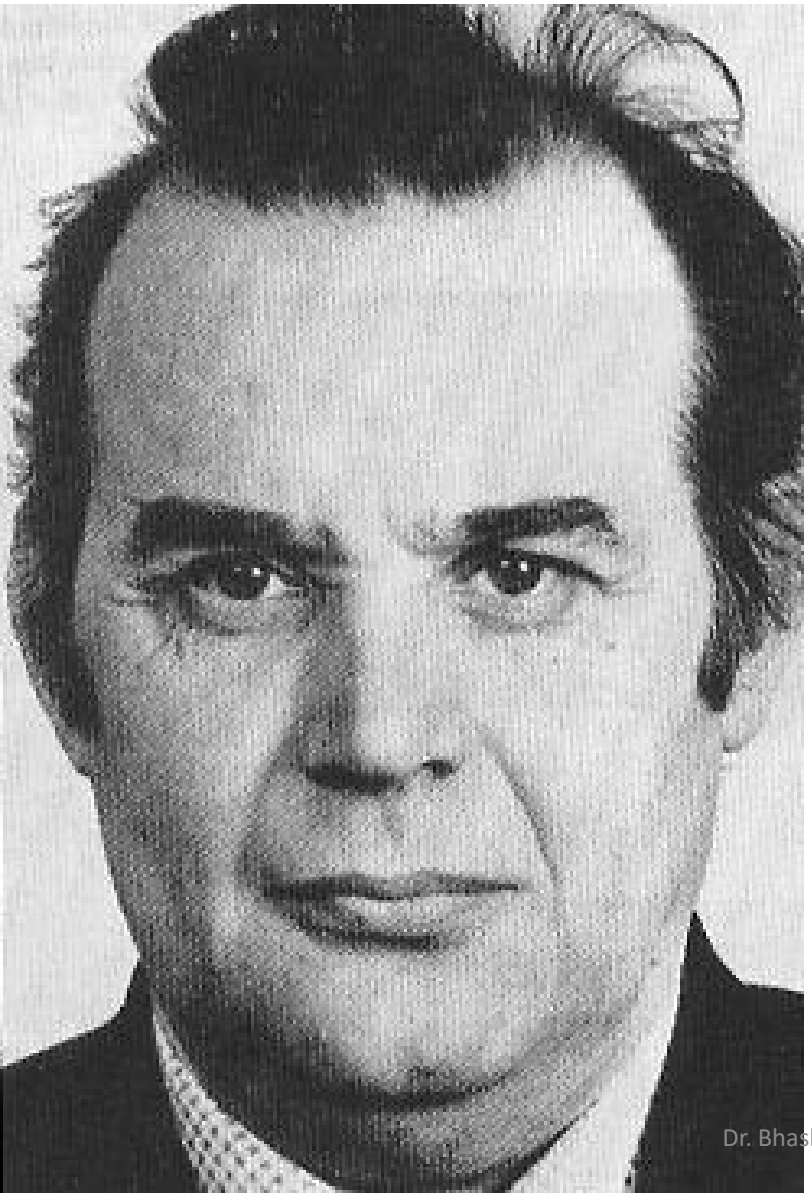
Policy evasion

Malicious file transfer

Command and control

Data exfiltration

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cs@gmail.com



The logic bomb - 1982

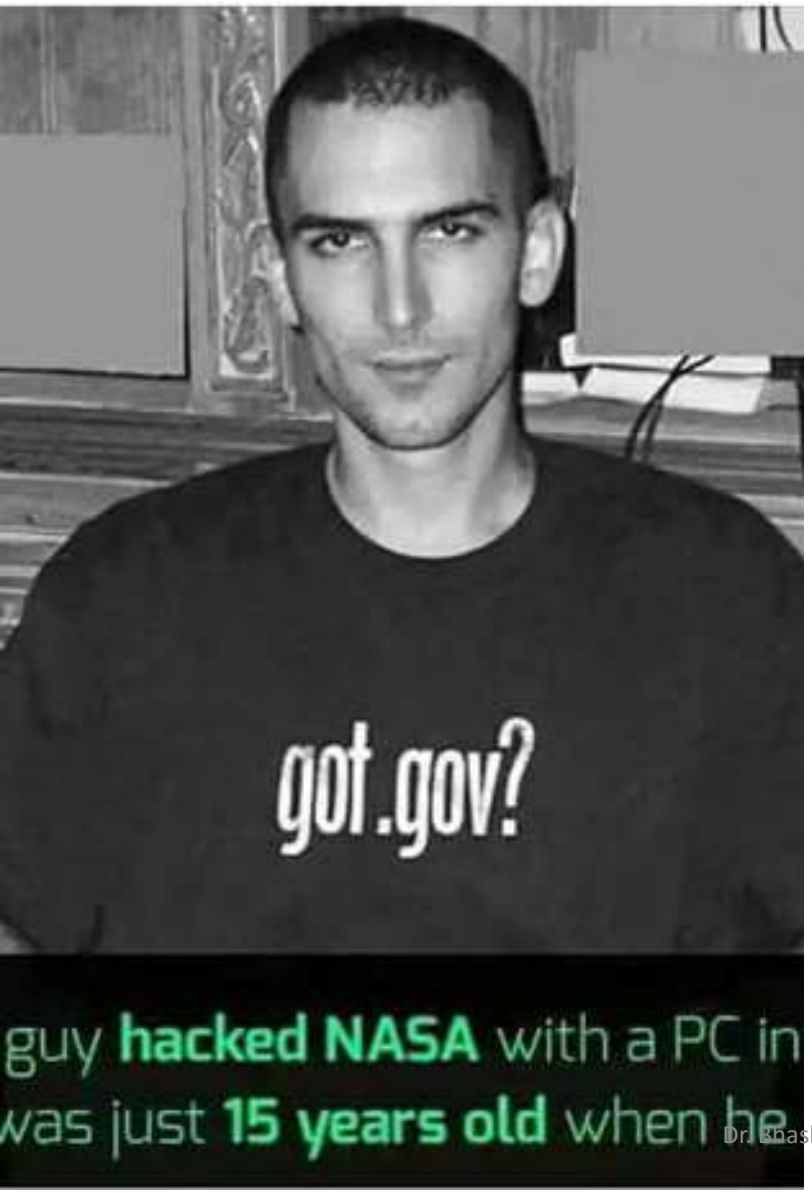
- Farewell Dossier (Vladimir Vetrov)
- Believed that an operation launched by CIA against a Russian pipeline
- Malicious code used to affect the pipeline and make it explode, without any actual explosive
- Damages could be seen from space.

Kevin Mitnick - 1983

- Kevin Mitnick gets inside the Pentagone's network.
- Motivated by the challenge
- Does not steal data and keeps a sense of ethics
- Works as an Information Security Consultant

Morris Worm - 1988

- Created par Robert T. Morris (Cornell) in 1988
- Morris wanted to measure the depth of Internet
- He designed a Software that would replicate itself and propagate forth and forth (Worm)
- However the worm encountered an error and caused damages to the memory of infected computers
- Over 6000 computer infected with a $100M fine
- Works as an investor at the Y Combinator



Jonathan James - 1999

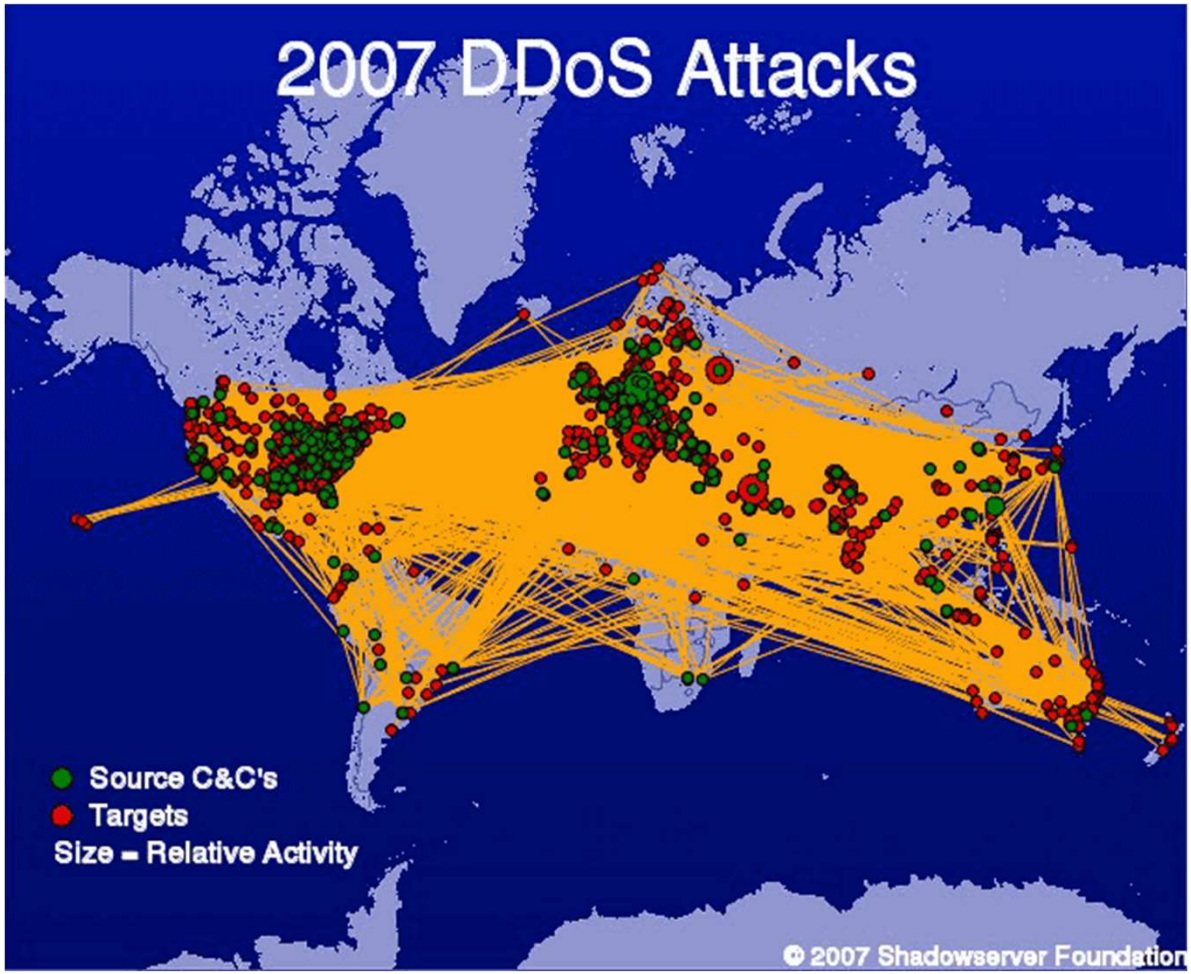
- Pirates the Defense Threat Reduction Agency at 15
- Installs a backdoor on a server, a sniffer, and steals access to military computers
- Gets the full source code of the ISS life control system
- Accused of several other unsolved attacks
- Commits suicide in 2008

MafiaBoy - 2000

- Michael Calce (aka MafiaBoy) launches DDoS attacks against major websites (Amazon, CNN, eBay, Yahoo!)
- Damages estimated over $1,2B
- Sells his skills as Information Security Consultant
- This event is considered as the “Pearl Harbor” of Information Security (Craig Guent, CIA)

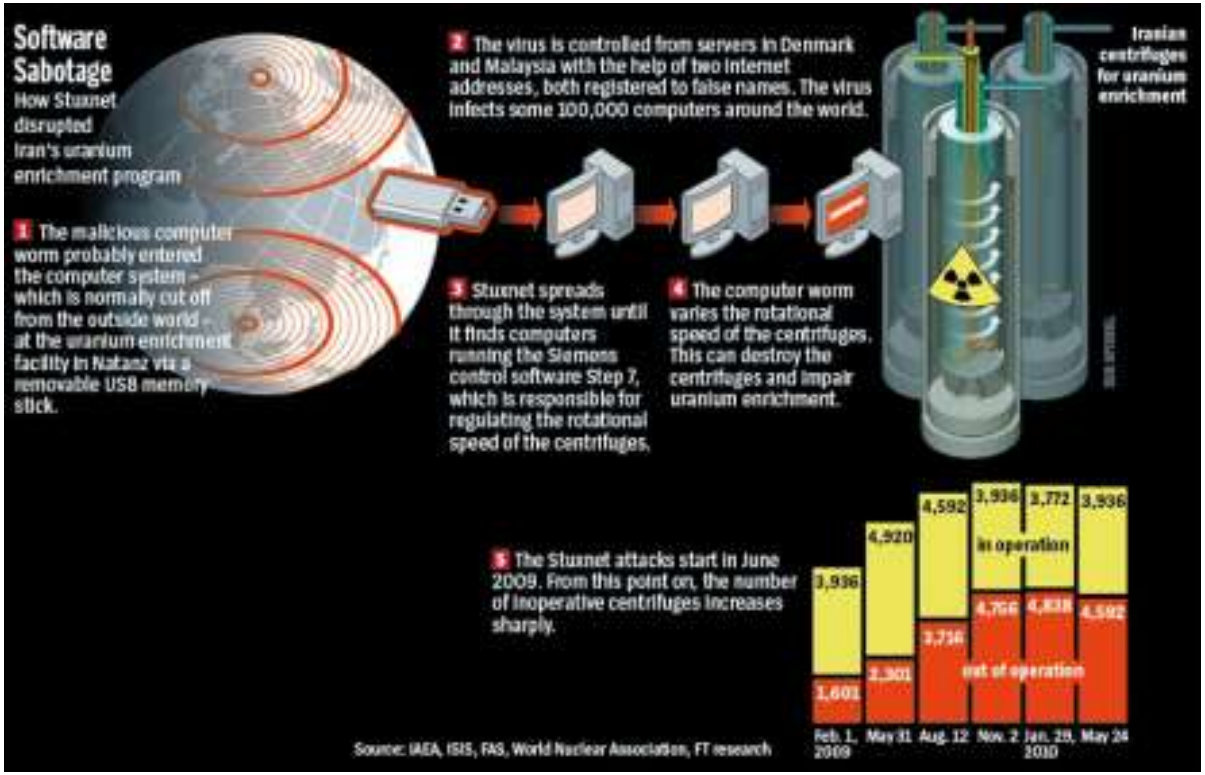
Estonia - 2007

- Estonia is targeted by a major DDoS attack following the removal of a russian war memorial.
- Governmental services were completely off.
- One of the first major political cyberattack against a country



StuxNet – 2009/2010

- High expertise virus targeting Siemens machines
- Sabotage against the Iran's nuclear program

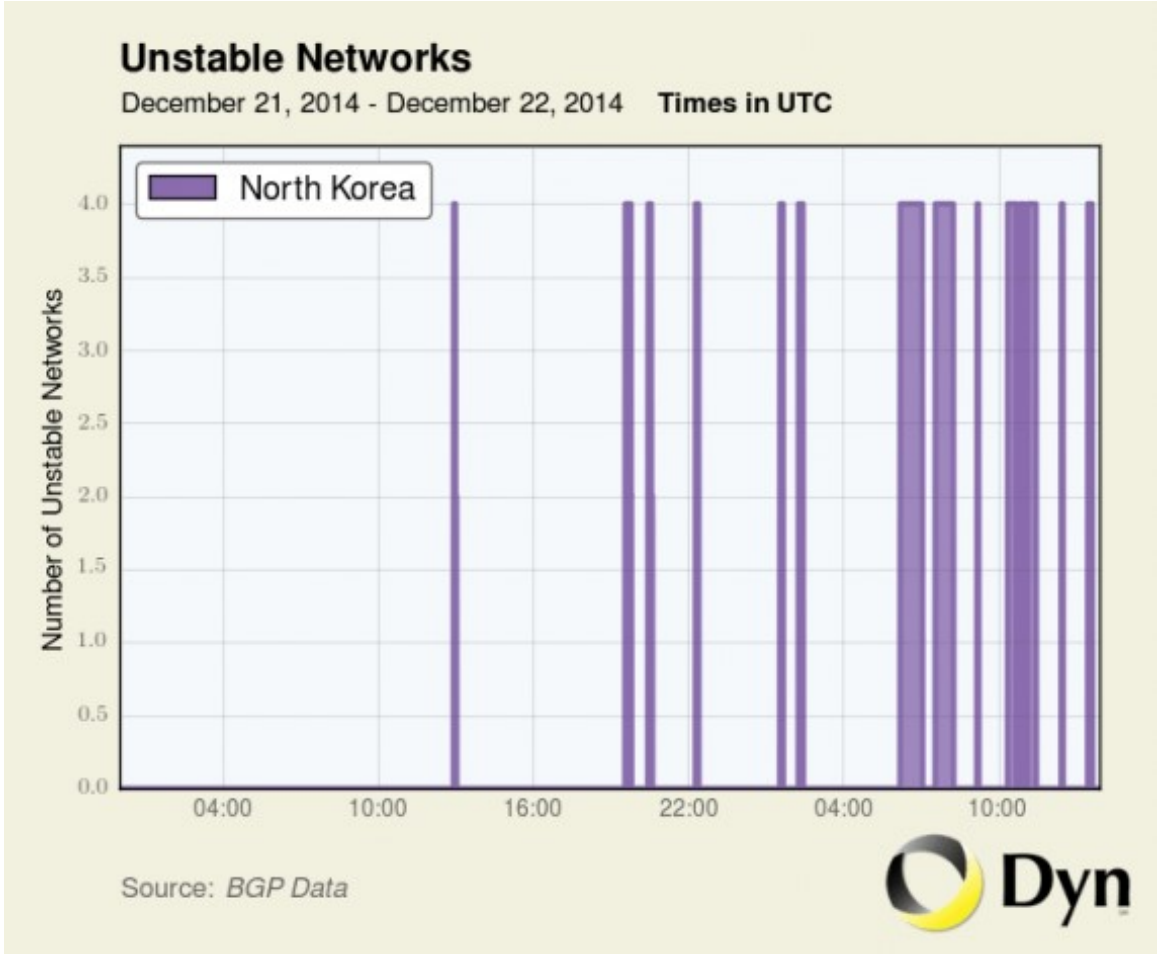


Sony Pictures Entertainment - 2014

- Major data theft orchestrated by North Korea
- Stolen movies were published on the Internet for free
- Damages estimated over $100M

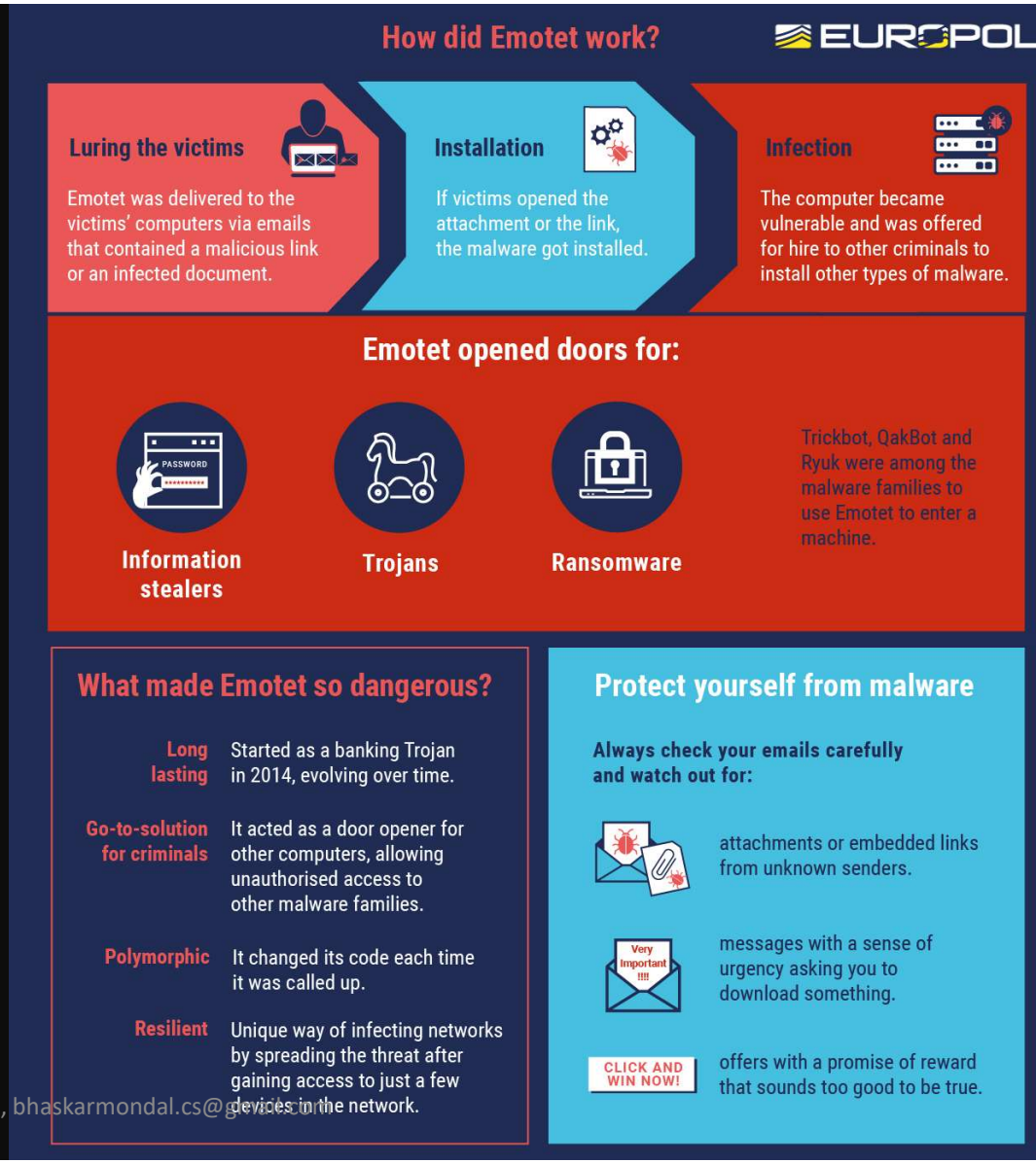
North Korean Internet Outage - 2014

- North Korea lost its Internet connection for 10 hours on December 23 2014
- This incident occurred right after the Sony Pictures Entertainment intrusion
- North Korea accused Washington
- USA officially declined any involvement



EMOTET

- most pervasive and dangerous botnets of the past decade: 'EMOTET'
- First discovered as a **banking Trojan in 2014**
- has been one of the most professional and long-lasting cybercrime services, ever to exist.
- data theft and extortion through ransomware.
- EMOTET employed a fully automated process to deliver infected email attachments to victims' computers
- hundreds of servers located across the world was used by EMOTET to conduct its operations
- These included managing the computers of the infected victims, launching new attacks, serving other criminal groups, and also make the network more resilient against takedown attempts.



And now?

- The Ransomware era
- Multiple Data breaches:
  - Ashley Madison
  - LinkedIn
  - Adobe
  - and so on…

3 aspects of information security: Services, Mechanisms, Attacks

- security attacks (and threats)
  - actions that (may) compromise security
- security services
  - services counter to attacks
- security mechanisms
  - used by services
  - e.g. secrecy is a service, encryption (a.k.a. encipherment) is a mechanism

Attack

- An attack occurs when someone attempts to exploit a vulnerability
- Type of attacks
  - Passive (e.g., eavesdropping)
  - Active (e.g., password guessing, DoS)
- A compromise occurs when an attack is successful

Key Information Security Concepts

- Computer can be subject or object of an attack
  - When the subject of an attack
    - An active tool to conduct attack
  - When the object of an attack
    - An entity being attacked

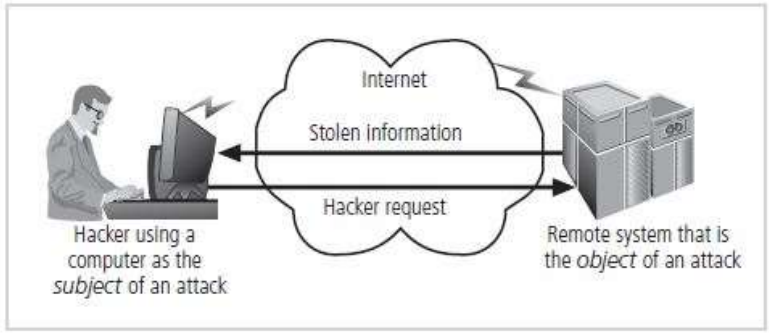
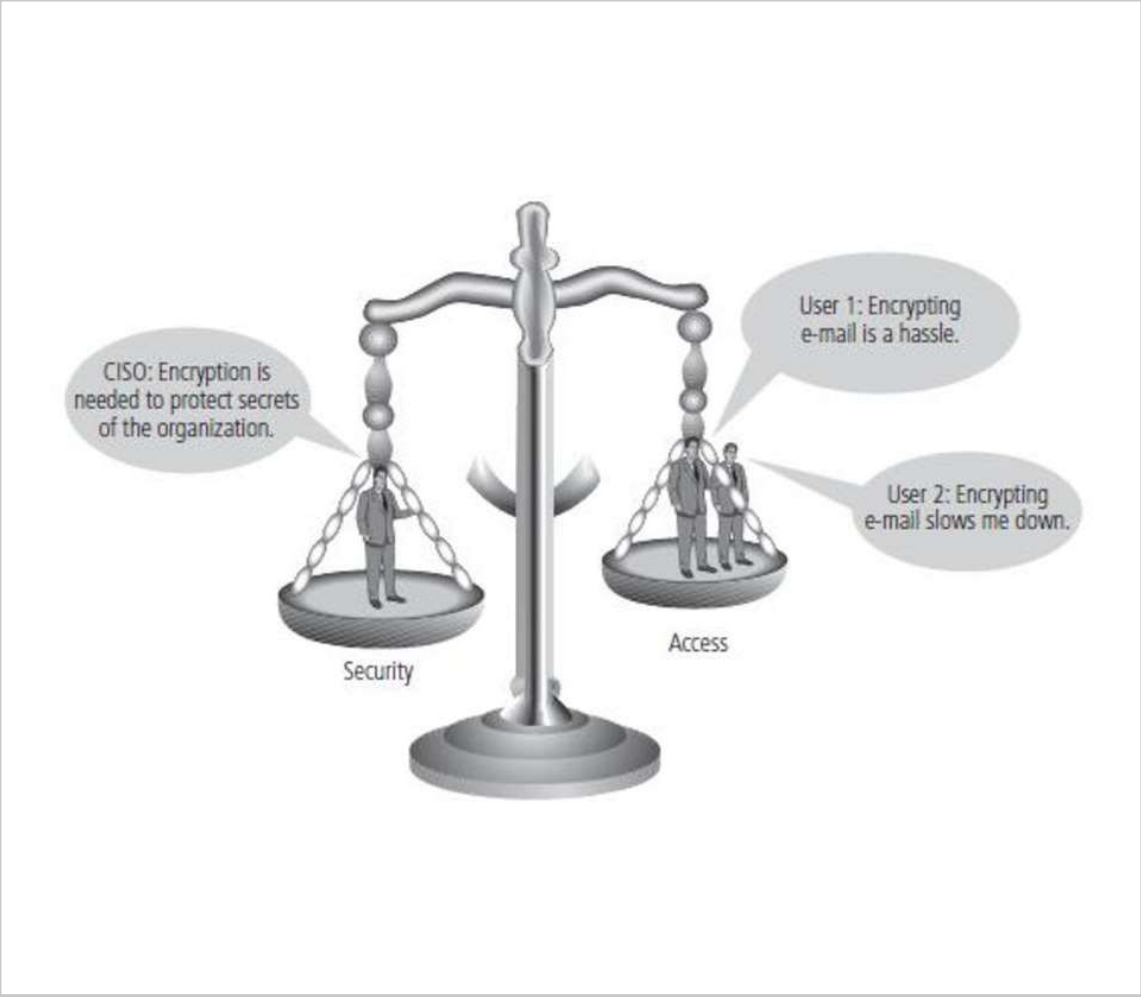


Figure 1-2 Computer as the subject and object of an attack

Dr. Bhaskar Mondal, NIT Patna, bhaskarmondal.cse@gmail.com

Information Security vs. Access

- Perfect security is impossible
- Security is a process
- Security should be considered balance between protection and availability
- Must allow reasonable access, yet protect against threats



Attacks

- Attacks on computer systems
  - break-in to destroy information
  - break-in to steal information
  - blocking to operate properly
  - malicious software
    - wide spectrum of problems
- Source of attacks
  - Insiders
  - Outsiders

Attacker Motives

Access	Influence	Profit
• Network • Application • Data	• Hactivism • Blackmail • Extortion • Reputation Damage	• Financial Transactions • Identity Theft • Ransom • Sell for Profit • Trade for Services

Attack Types

Tools or Software	Technical	Non-Technical
• Exploit Kits • Tool Kits • Keyloggers • Banking Trojans • Phishing	• Vulnerabilities • Exploits • Brute Force • DNS Hijacking • Vulnerabilities • Input Capture • Sniffing	• Phishing • Social Engineering • Stolen Credentials • Social Engineering • Dumped Databases • Leaked Credentials

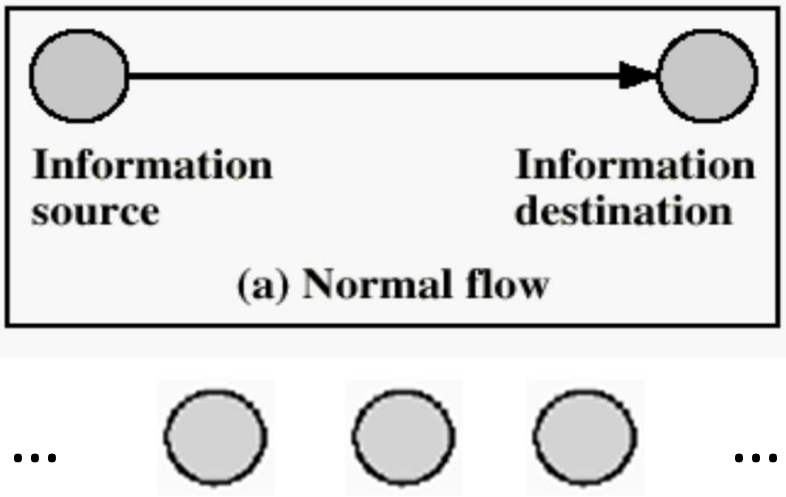
Evolution Of Cyber Security

- Viruses (1990s) Anti-Virus, Firewalls
- Worms (2000s) Intrusion Detection & Prevention
- Botnets (late 2000s to Current) DLP, Application-aware Firewalls, SIM
- APT, Insiders (Current) Network Flow Analysis

Defense Considerations

Implement multi-factor authentication	Segment your network environment	Enforce “least privilege” and segregation of duties	Implement network activity and data leak monitoring
Prioritize patching	Segment your network environment	Enforce secure coding	Implement application gateway firewalls
	Perform regular vulnerability scanning	Train employees to be vigilant against phishing attacks	

Security Threats / Attacks



Security Threats / Attacks

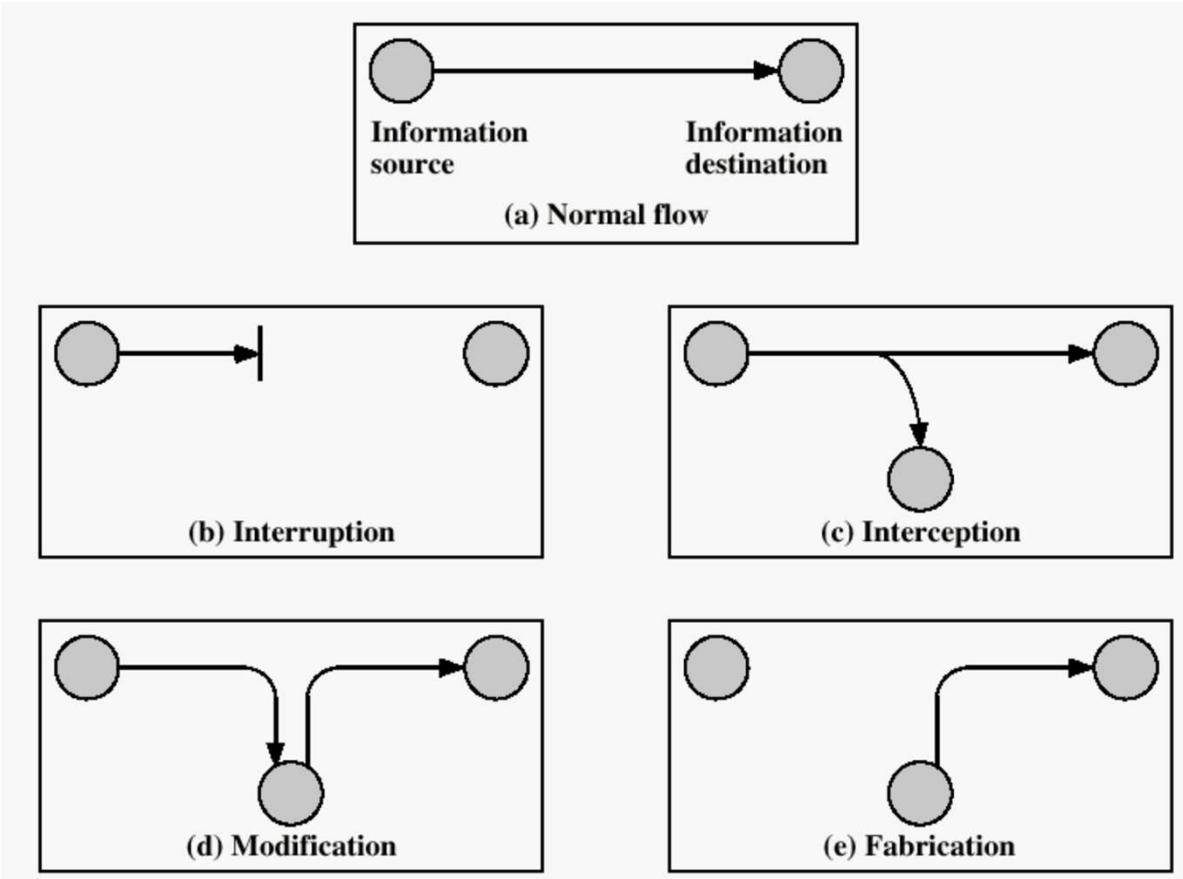


Figure 1.1 Security Threats

Passive Attacks

- Passive attacks
  - interception of the messages
  - What can the attacker do?
    - use information internally
      - hard to understand
    - release the content
      - can be understood
    - traffic analysis
      - hard to avoid
  - Hard to detect, try to prevent

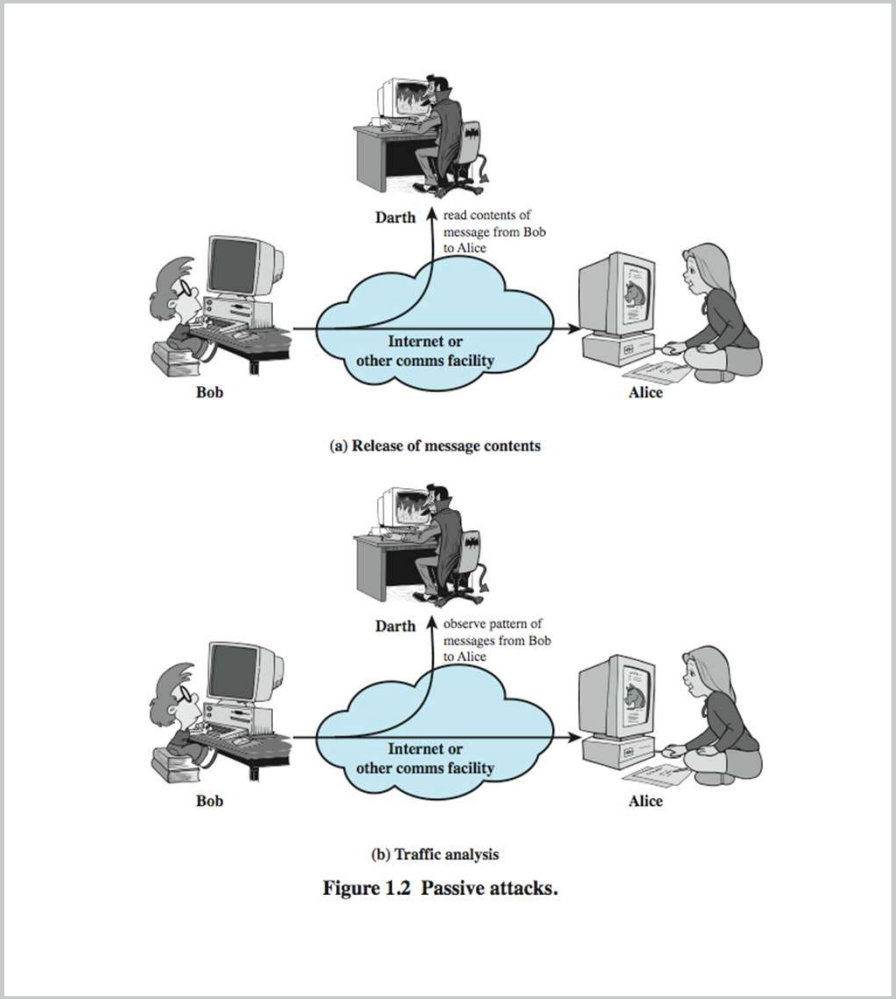
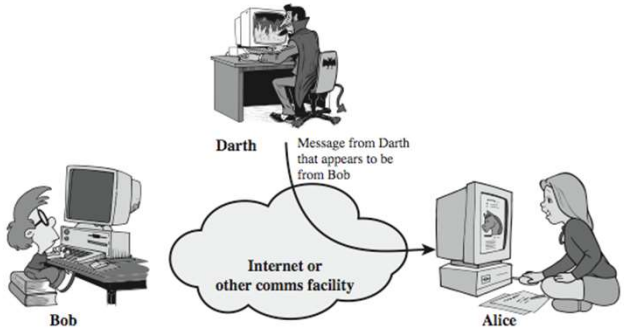


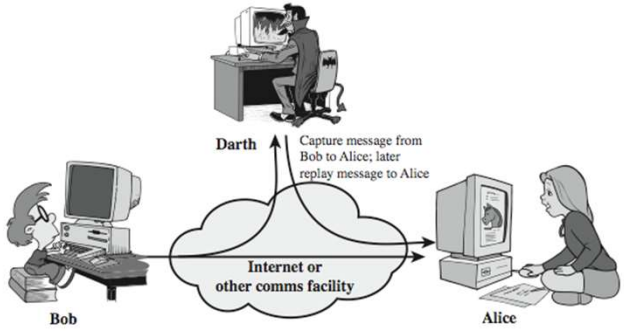
Figure 1.2 Passive attacks.

Active Attacks (1)

- Active attacks
  - Attacker actively manipulates the communication
  - Masquerade
    - pretend as someone else
    - possibly to get more privileges
  - Replay
    - passively capture data and send later
  - Denial-of-service
    - prevention the normal use of servers, end users, or network itself



(a) Masquerade

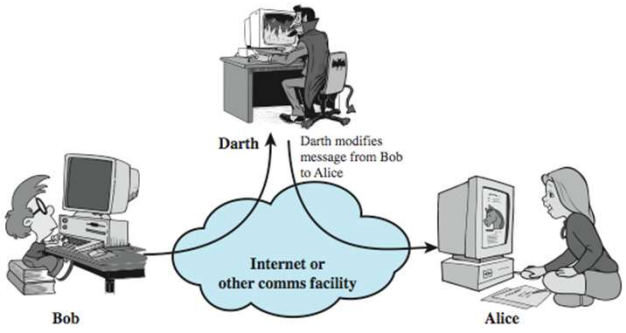


(b) Replay

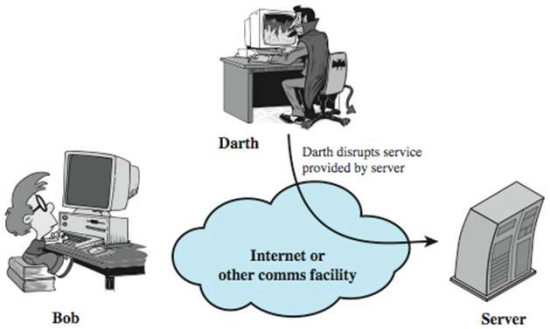
Figure 1.3 Active attacks (page 1 of 2)

Active Attacks (2)

- Active attacks (cont'd)
  - deny
    - repudiate sending/receiving a message later
  - modification
    - change the content of a message



(c) Modification of messages



(d) Denial of service

Figure 1.3 Active Attacks (page 2 of 2)

Security Services

- to prevent or detect attacks
- to enhance the security
- replicate functions of physical documents
  - e.g.
    - have signatures, dates
    - need protection from disclosure, tampering, or destruction
    - notarize
    - record

Model for Network Access Security

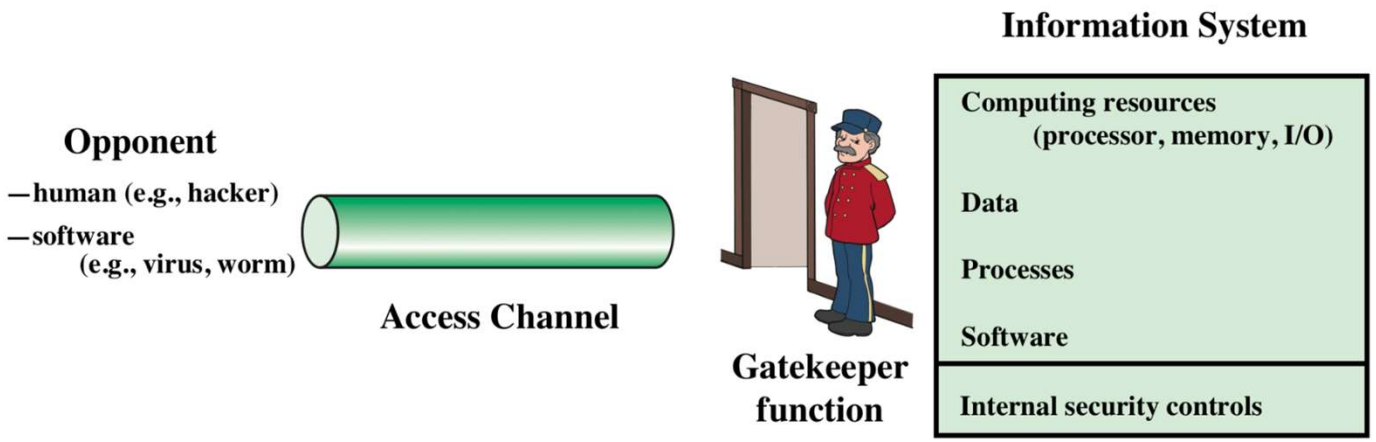


Figure 1.3 Network Access Security Model

Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users and processes and ensure only authorized users and processes access designated information or resources
  - Internal control to monitor the activity and analyze information to detect unwanted intruders

Dr. Bhaskar Mondal, NIT Patna,
bhaskarmondal.cs@gmail.com

About NIST and Standards

- “Founded in 1901 NIST, the National Institute of Standards and Technology, (former NBS) is a nonregulatory federal agency within the U.S. Commerce Department’s Technology Administration.
- NIST‘s mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.”
- Cryptographic Standards & Applications.
- Federal Information Processing Standards (FIPS): define security standards

More on Computer System Security

- Based on “Security Policies”
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements
    - Which actions are permitted, which are not
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - Partially automated, but mostly humans are involved
  - Assurance and Evaluation
    - Assurance: degree of confidence to a system
    - Security products and systems must be evaluated using certain criteria in order to decide whether they assure security or not

Attack Surfaces

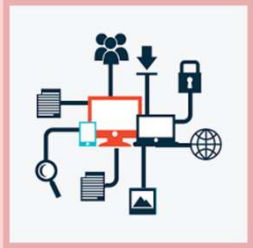
- An attack surface consists of the reachable and exploitable vulnerabilities in a system
- Examples:
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available in a firewall
  - Code that processes incoming data, email, XML, office documents, etc.
  - Interfaces and Web forms
  - An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

- Network attack surface
  - Refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
    - E.g. DoS, intruders exploiting network protocol vulnerabilities
- Software attack surface
  - Refers to vulnerabilities in application, utility, or operating system code
- Human attack surface
  - Refers to vulnerabilities created by personnel or outsiders
  - E.g. social engineering, insider traitors

Dr. Bhaskar Mondal, NIT Patna,
bhaskarmondal.cs@gmail.com

Anatomy of Attack

1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective/ Resources	Data Gathering/ Target Identification	Identify Vulnerabilities / Scanning/ Enumaration	Gain Access/ Create Foothold	Gane Escalated Privilages/ Root Access	Multiple Footholds/ Paths/ Backdoors	Obfuscate Presence	Exploit/ Exfiltaration/ Attack to Achieve Objective
							

Fundamental Dilemma of Security

- **“Security unaware users have specific security requirements but no security expertise.”**
  - from D. Gollmann
  - Solution: level of security is given in predefined classes specified in some common criteria
    - Orange book (Trusted Computer System Evaluation Criteria) is such a criteria

Dr. Bhaskar Mondal, NIT Patna,
bhaskarmondal.cs@gmail.com

Fundamental Tradeoff

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes

"If security is an add-on that people have to do something special to get, then most of the time they will not get it"

Martin Hellman,

co-inventor of Public Key Cryptography

Good Enough Security

"Everything should be as secure as necessary, but not securer"

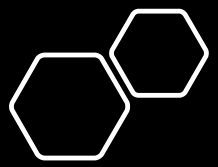
Ravi Sandhu, "Good Enough Security", IEEE Internet Computing, January/ February 2003, pp. 66- 68.

- Read the full article at

http://dx.doi.org/10.1109/MIC.2003.1167341

Information Security and Cryptography Technologies

System Security Technology	Network Security Technology	Wireless Network Security Technology	Cryptography
• Protecting Peripheral Components • Protecting Distributed Contents • Trusted Computing Platforms • Detecting Intrusion/ Malware • Protecting Data/Access Control • Authentication	• Protecting Privacy or Anonymity • IEEE 802.11 • Security Pairing	• Security at particular protocol layers • Detecting Malicious traffic • Key Management	• Symmetric Cypher • Asymmetric Cypher • PKI-Digital certificate • Secure hashing • Key Management • Quantum Cryptography



Some Other Security Facts

- Not as simple as it might first appear to the novice
- Must consider all potential attacks when designing a system
- Generally yields complex and counterintuitive systems
- Battle of intelligent strategies between attacker and admin
- Requires regular monitoring
- Not considered as a beneficial investment until a security failure occurs
  - Actually security investments must be considered as insurance against attacks
- too often an afterthought
  - Not only from investment point of view, but also from design point of view

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education